REMARKS

Claims 1-8 are pending in this application. In this Amendment, Applicants have canceled claims 9-19 from further consideration in this application. Applicants are not conceding that the subject matter encompassed by claims 9-19, prior to this Amendment, are not patentable over the art cited by the Examiner. Claims 9-19 were cancelled in this Amendment solely to facilitate expeditious prosecution of the subject matter of the remaining claims. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by claims 9-19, as presented prior to this Amendment, and any additional claims, in one or more continuing applications. Reconsideration of the claims in view of the following remarks is respectfully requested.

I. Examiner's Response to Applicants' Arguments filed August 29, 2007

Responsive to the Office Action dated May 29, 2007, Applicants filed a Response on August 29, 2007 as opposed to the July 3, 2007 date stated by the Office Action. The present Office Action provides rebuttal comments to Applicants' arguments presented in the Response filed August 29, 2007. While Applicants recognize these arguments with regard to the combination of the Atkinson and O'Donnell references, Applicants further recognize that the Office Action changes the rejection to a combination of Atkinson and Riggins. Thus, Applicants respectfully submit that any arguments with regard to the combination of Atkinson and O'Donnell are moot and Applicants will direct any arguments solely to the currently applied combination of references.

II. 35 U.S.C. § 103, Alleged Obviousness, Claims 1 and 8-19

The Office Action rejects claims 1 and 8-19 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Atkinson et al. (U.S. Patent No. 6,367,012 B1) in view of Riggins (U.S. Patent No. 6,766,454 B1). This rejection is moot with regard to canceled claims 9-19 and is respectfully traversed with regard to the remaining claims.

Claim 1 reads as follows:

1. A method of authenticating a digitally encoded product being originated by an entity having at least one authorized subject, the method including the steps of:

a client system transmitting a request of authentication of the product to a server system,

the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification:

certifying that the product originates from the entity using sensitive information of the entity stored on the server system, and

returning a representation of the certification to the client system. (emphasis added)

The Office Action bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Applicants respectfully submit that Atkinson and Riggins, taken alone or in combination, fail to teach or suggest a client system that transmits a request of authentication of a product to a server system and a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system and returns a representation of the certification to the client system. Since the references fail to teach or suggest these features, the Office Action has failed to establish a *prima facie* case of obviousness because the Office Action does not show where each and every claim limitation is taught or fairly suggested by the applied prior art.

Atkinson is directed to providing an executable file that incorporates a certification or signature to assure its authenticity and integrity, particularly for those executable files that are received at a recipient's computer over an open computer network like the Internet. Atkinson's executable file includes a publisher digital certificate that is attached to a publisher signature. The publisher digital certificate is issued by a certification authority or agency to authenticate the identity of the publisher issuing the publisher signature. The digital certificate is encrypted with a private key corresponding to a widely known and readily available certification agency public key on the recipient's computer. This certification of the executable file or code is confirmed or read at the recipient's computer.

The Office Action alleges that Atkinson teaches a client system transmitting a request of authentication of the product to a server system in column 7, lines 52-67, which is reproduced as follows:

> FIG. 6 is a flow diagram representing a publisher signature confirmation method 150 that is performed, for example, by or in response to a call by browser application 138. Signature confirmation method 150 provides a recipient of executable file 102 (FIG. 4) with simple and effective assurance of the authenticity and integrity of executable file 102.
>
> Process block 152 indicates that a user receives an executable computer program file via an open network like the Internet.
>
> Decision block 154 represents an inquiry as to whether the executable file includes a publisher signature 110. For example, browser application 138 searches the received executable file or its header (as described below in greater detail) for a publisher signature in the form of a cryptographic message of a conventional standard such as, for example, PKCS #7 version 1.5, promulgated by RSA Laboratories. Whenever a publisher signature is not included in the program file, decision block 154 proceeds to process block 156, and otherwise proceeds to process block 158.
>
> Process block 156 indicates that a dialog or notice is rendered notifying the user of the absence of a publisher signature in the program file 138. The dialog can be rendered by browser application 138, for example, and can include user queries as to whether to open or run executable file 102.

(Atkinson, column 7, line 52, to column 8, line 9)

In this section, Atkinson describes that a user receives an executable file via an open network like the Internet. Upon the user inquiring as to whether the executable file includes a publisher signature, a browser application **searches the received executable file or its header** for a publisher signature in the form of a cryptographic message of a conventional standard. If there is not a publisher signature included in the executable file, the Atkinson system renders a dialog or notice **notifying the user of the absence of a publisher signature**. The rendered dialog can include user queries as to whether to open or run the executable file. Thus, Atkinson performs all of these tasks on the recipient's computer and, if the digital signature is not included, Atkinson merely notifies the user that the digital signature is not provided. Therefore, Applicants respectfully submit that Atkinson fails to teach or suggest a client system that **transmits** a request of authentication of the product **to a server system**.

The Office Action further states:

> The Examiner disagrees with argument and notes that Atkinson teaches a client that transmits a request of authentication of a product to a server system, note the Examiner interprets this request equivalent to browser that can be integrated with an operating system network to communicate with a remote computer (i.e. a server) in col. 5, lines 36-58 as well as col. 7, lines 52-67 the call by the browser application for signature confirmation. Note the client request is interpreted to be equivalent 'a call from the browser application' and the 'inquiry as to whether the executable file includes a publisher signature'. Note Atkinson teaches that the browser communicates with remote computers, the calls to these remote computers that deliver products that contain a publisher signature are interpreted to be equivalent to authentication of a product from a 'server system'.

(Office Action dated November 9, 2007, pages 2-3)

While Atkinson may describe, in column 5, lines 36-58, that a browser on a computer may communicate via a remote computer network, such as the Internet, the browser of Atkinson is integrated into the operating system of the user's computer or is a separate application software running on the user's computer and is not a server system. The Office Action seems to acknowledge that the browser is not a server system by stating that the browser communicates with a remote computer which the Office Action relates to a server system. However, even if the remote computer is a server system, Applicants respectfully submit that Atkinson would have no need to transmit a request of authentication of a product to the server system. That is, as discussed above, the user of Atkinson receives an executable file via an open network like the Internet. Upon the user inquiring as to whether the executable file, **which the user has already received on the user's computer**, includes a publisher signature, the browser application **on the user's computer** searches **the received executable file or its header** for a publisher signature in the form of a cryptographic message of a conventional standard. Thus, even if the browser of Atkinson can communicate via a remote computer network, there would be no need for the browser of Atkinson to make a call to the remote computer network, since **the executable file is already on the user's computer** and the browser checks **the received executable file** for the digital signature. Therefore, Applicants respectfully submit that Atkinson fails to teach or suggest a client system that **transmits** a request of authentication of the product **to a server system**.

Moreover, Atkinson does not teach or suggest a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system. The Office Action acknowledges that Atkinson does not teach or suggest this feature. However, the Office Action alleges that Riggins teaches this feature.

Riggins is directed to identifying and authenticating a user in a computer network. Upon receiving a request for access, the server of Riggins sends an authentication applet to the client. The authentication applet includes a user identification (ID) module for obtaining a user ID and a password module for obtaining a client password. The authentication applet also includes a response generator coupled to the password module for using the client password as a variable in an algorithm to compute a client response. The authentication applet further includes a communications module coupled to the response generator and to the user ID module for sending the client response and the user ID back to the server for verifying the response and authenticating the user. The server uses the user ID to retrieve user information, and uses the user information as a variable in an algorithm to generate a verification response. If the verification response is the same as the client response, then the identity of the user is verified and access may be granted.

Thus, Riggins teaches granting access to a server for a user using an authentication applet and by identifying and authenticating **the user**. In contradistinction, the present application is directed to a server system that certifies that **a product originates from an entity** using sensitive information of the entity stored on the server system. That is, the present application certifies that **the product** that the client is attempting to authorize **originates from an entity** rather than merely granting access to a server. Nowhere, in any section of Riggins, is there a teaching or suggestion of certifying that **the client application originates from any entity**. Riggins merely describes that a user is authenticated using an authentication application.

The Office Action alleges that Riggins teaches a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system in column 2, lines 36-62, which is reproduced as follows:

> The present invention provides a system and method for authenticating the identity of a user in a computer network. The network system includes a server coupled via a computer network to a client. Upon

> receiving a request for access, the server sends an authentication applet to the client. The authentication applet includes a user identification (ID) module for obtaining a user ID and a password module for obtaining a client password. The authentication applet also includes a response generator coupled to the password module for using the client password as a variable in an algorithm to compute a client response. The authentication applet further includes a communications module coupled to the response generator and to the user ID module for sending the client response and the user ID back to the server for user authentication. The client uses an applet engine to execute the applet. The server uses the received user ID, the response and possibly user information to verify the identity of the user.
>
> The method includes the steps of receiving a service request from a client, delivering to the client an authentication applet which when executed by the client uses client input as a variable in an algorithm to compute a response, receiving the response and a user ID from the client, and verifying the response. Verifying the response includes using the user ID and the challenge and possibly user information to verify the user.

(Riggins, column 2, lines 36-62)

In this section, Riggins describes receiving a request for access from a user and sending an authentication applet to the client. The authentication applet obtains a user ID and client password. The authentication applet uses the client password as a variable in an algorithm to compute a client response. The authentication applet sends the client response and the user ID back to the server for verifying the response and authenticating the user. The server uses the user ID to retrieve user information, and uses the user information as a variable in an algorithm to generate a verification response. If the verification response is the same as the client response, then the identity of the user is verified and access to the server is granted. Applicants respectfully submit that authenticating a user so that a user may access a server is not equivalent to certifying that **a product originates from the entity using sensitive information of the entity stored on the server system**. That is, the user does not send a request for authentication of a product to the Riggins server. The user of Riggins merely sends a request for access to a server.

Further, the Office Action alleges that Atkinson teaches returning a representation of the certification to the client system in column 8, lines 45-63, which is reproduced as follows:

> Process block 170 indicates that the recipient computer selectively renders a dialog 180 (FIG. 7) confirming the certification of the received code or executable file. The rendering of the dialog is selective in that the recipient can prevent dialog 180 from being rendered, for example, for particular certification agencies or publishers selected by the recipient or user as being trusted software publishers.
>
> FIG. 7 illustrates an exemplary digital certificate dialog 180 rendered on a display screen associated with the recipient computer 20 in accordance with process block 170 of signature confirmation method 150. Dialog 180 provides a user with a simple two-part identity confirmation of the publisher of executable file 102. More specifically, dialog 180 identifies the executable file 102 as having been "published by Publisher under an Internet publishing license granted by Agency." This identification of the Publisher with confirmation by the Agency or certification Agency provides the user with simple and effective authentication.

(Atkinson, column 8, lines 45-63)

In this section, Atkinson describes that the executable code that has be downloaded on the recipient's computer, when executed, will render a dialog that confirms the certification of the executable file. However, the certification is received **with the executable file**. The certification of Atkinson is not received in response to a request sent by a client system **to a server system** that requests authorization of the product. As discussed above, Atkinson performs all operation on the recipient's computer and that, if a digital signature is not received, Atkinson merely renders a dialog or notice **notifying the user of the absence of a publisher signature** and querying the user as to whether to open or run the executable file.

Similar distinctions of the claims over the cited references apply to independent claim 8. Claim 8 recites "**a client system transmitting a request of authentication of the product to a server system**, the server system verifying whether the request is received from an authorized subject, and responsive to a positive verification: **generating a digital signature of the product using a private key of the entity stored on the server system**, and **returning the digital signature to the client system, wherein the digital signature certifies that the product originates from the entity**." (emphasis added). Again, Atkinson and Riggins, taken alone or in combination, fail to teach or suggest a client system that transmits a request of authentication of the product to a server system, a server system that certifies that the product originates **from an entity** using

sensitive information of the entity stored on the server system, and a server system that returns a representation of the certification to the client system.

Furthermore, no suggestion is present in any of the references to modify the references to include such a feature. That is, there is no teaching or suggestion in Atkinson or Riggins, taken alone or in combination, that a problem exists for which transmitting from a client system a request of authentication of the product to a server system, certifying by a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system, is a solution. To the contrary, Atkinson merely determines if a digital signature is included with an executable file that is downloaded to a recipient's computer and, if not, presents a dialog notifying the recipient that the digital signature is missing. Riggins merely teaches authenticating a user so that the user may access a server. Neither of the references certifies at a server system that **a product** originates **from an entity** using sensitive information of the entity stored on the server system.

Moreover, neither reference teaches or suggests the desirability of incorporating the subject matter of the other reference. That is, there is no motivation offered in either reference for the alleged combination. The Office Action alleges that the motivation would be "because of the need for subscriber data management." The present invention provides for a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system. As discussed above, Atkinson merely determines if a digital signature is included with an executable file that is downloaded to a recipient's computer and Riggins merely teaches authenticating a user so that the user may access a server. Neither reference teaches or suggests transmitting a request of authentication of the product to a server system, a server system that certifies that the product originates from the entity using sensitive information of the entity stored on the server system, and a server system returning a representation of the certification to the client system. Thus, the only teaching or suggestion to even attempt the alleged combination is based on a prior knowledge of Applicants' claimed invention thereby constituting impermissible hindsight reconstruction using Applicants' own disclosure as a guide.

One of ordinary skill in the art, being presented only with Atkinson and Riggins, and without having a prior knowledge of Applicants' claimed invention, would not have found it obvious to combine and modify Atkinson and Riggins to arrive at Applicants' claimed invention, as recited in claim 1. To the contrary, even if one were somehow motivated to combine Atkinson and Riggins, and it were somehow possible to combine the systems, the result would not be the invention as recited in claim 1. The resulting system would be verifying that a user has access to download the executable file prior to downloading the file. The resulting system would still fail to transmit a request of authentication of the product to a server system, certify at a server system that the product originates from the entity using sensitive information of the entity stored on the server system, and return from a server system a representation of the certification to the client system.

In view of the above, Applicants respectfully submit that Atkinson and Riggins, taken alone or in combination, fail to teach or suggest the features of claims 1 and 8-19. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1 and 8-19 under 35 U.S.C. § 103(a).

III. 35 U.S.C. § 103, Alleged Obviousness, Claims 2-7

The Office Action rejects claims 2-7 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Atkinson et al. (U.S. Patent No. 6,367,012 B1) in view of Riggins (U.S. Patent No. 6,766,454 B1) in further view of O'Donnell et al. (U.S. Patent No. 7,024,689 B2). This rejection is respectfully traversed.

Claims 2-7 are dependent on independent claim 1 and, thus, these claims distinguish over Atkinson and Riggins for at least the reasons noted above with regard to claim 1. Moreover, O'Donnell does not provide for the deficiencies of Atkinson and Riggins and, thus, any alleged combination of Atkinson, Riggins, and O'Donnell would not be sufficient to reject independent claim 1 or claims 2-7 by virtue of their dependency. That is, Atkinson, Riggins, and O'Donnell, taken alone or in combination, do not teach or suggest transmitting from a client system a request of authentication of the product to a server system, certifying by a server system that the product originates

from the entity using sensitive information of the entity stored on the server system, and returning by a server system a representation of the certification to the client system.

Furthermore, Atkinson, Riggins, and O'Donnell, taken alone or in combination, fail to teach or suggest the features of claims 2-7. For example, with regard to claim 4, Atkinson, Riggins, and O'Donnell, taken alone or in combination, do not teach or suggest automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key. The Office Action acknowledges that Atkins and Riggins do not teach these features, but alleges that O'Donnell teaches automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key.

O'Donnell is directed to an access site that allows a client application to access a server application on behalf of a subscriber who has an account at the client site. When the subscriber registers the client application with the access site, the subscriber also specifies access rights to the access site and issues a certificate in association with the specified access rights. The access site sends the certificate to the client application. When a user wants to access the features of the client application that integrate with the server application, the client application issues the certificate to the user and the access site. Then, the client application redirects the user to the access site. When the user accesses the access site, the user forwards the certificate to the access site. If the certificate from the user matches the certificate from the client application, then the access site validates the access and returns the results to the client application, whereupon the user is able to access the features of the client application that integrate with the server application.

The Office Action alleges that O'Donnell teaches automatically retrieving a private key of the entity stored on the server system, and digitally signing the product using the private key in column 2, line 63, to column 3, line 3, and column 3, lines 25-41, which are reproduced as follows:

> In one embodiment, the present invention allows subscribers to grant access rights to a client application in a system where a subscriber uses a client application to access a server application. An access site accommodates the granting of access rights, acting as a neutral broker between the client and server applications.

> Initially, application developers correspond with the access site to reserve names and receive corresponding certificates for client applications that they develop. These certificates are subsequently used as part of securely granting access to the server application by the client application. Specifically, the certificate is used to ensure that subsequent communications securely originate from the client application.
>
> A subscriber navigates to the client application (typically residing at a web site referred to as a client site), and requests features of the client application that implement the server application. This request can be variously made. For example, it can be a selection of a server application based feature that is presented at the client site, part of a more formal registration, and the like.
>
> After such a request, the subscriber is taken through steps that allow the subscriber to grant permission to a client application to access the server application. The granted permission can be variously defined. For example, the subscriber may grant permission for a payroll application to access an accounting application. However, the subscriber may not want the payroll application to be able the access certain accounting data. Further, the subscriber may want to require an authorized user to login prior to granting a request to process subscriber data.

(O'Donnell, column 2, line 57, to column 3, line 20)

> When the subscriber requests client application features that integrate with the server application, the client application gives the subscriber a unique confirmation code. Separately, the client application transmits the same confirmation code to the access site. The client application also causes the subscriber to be redirected to the access site with the confirmation code. The access site compares the confirmation codes received from the subscriber and the client application, verifying that they match, and thereby verifying that the subscriber is legitimately seeking to contact the server application based upon the previous exchange with the client application. Preferably, the confirmation code is sent by the client application to the server application using a security mechanism (e.g., SSL) that implements the previously issued certificate. This provides assurance to the server application that the confirmation code has been sent by the client application.

(O'Donnell, column 3, lines 25-41)

In column 2, line 63, to column 3, line 3, O'Donnell describes that application developers register their client application with an access site to reserve names and receive corresponding certificates for the client application. When a user wants to access the client application, the client application sends the certificate to the user and the access site. Then, the client application redirects the user to the access site. The user provides

the certificate received from the client application to the access site and the access site compares it to the certificate the access site receives from the client application. O'Donnell teaches that the certificate is used **to ensure that subsequent communications securely originate from the client application**. In column 3, lines 25-41, O'Donnell describes when a subscriber requests client application features that integrate with the server application, the client application gives the subscriber a unique confirmation code and, separately, the client application transmits the same confirmation code to the access site. The subscriber is redirected by the client application to the access site with the confirmation code. The access site compares the confirmation codes received from the subscriber and the client application, verifies that they match, and thereby verifies that the subscriber is legitimately seeking to contact the server application based upon the previous exchange with the client application.

Applicants respectfully submit that O'Donnell's access site does not automatically retrieve a private key of the entity from which the product originates that is stored on the server system. That is, O'Donnell's access site receives a certificate from the client application that **ensures that subsequent communications securely originate from the client application**. The certificate does not certify that the client application originated from an entity that originated the client application.

Additionally, with regard to claim 7, Atkinson, Riggins, and O'Donnell, taken alone or in combination, do not teach or suggest the client system invoking a remote command on the server system, the server system verifying whether the remote command is included in a predefined list stored on the server system, the list including at least one remote command for satisfying the request of authentication, and the server system executing the remote command if included in the list. The Office Action alleges that O'Donnell teaches this feature in column 10, lines 18-38, which is reproduced as follows:

> The client site provides web pages for interfacing with potential subscribers. As described above, a subscriber may navigate to a page pertaining to a client application and indicate 210 that he would like to use features of the client application that integrate with the server application. Pursuant to such an indication, an approved subscriber verification phase 208 provides confirmation that a subscriber contacting the server application is a legitimate user of the client application. Particularly, upon receipt of the indication that the subscriber would like to use such features, the client application generates a confirmation code that is sent 212 to the

> subscriber. The confirmation code can be any unique piece of information, typically dictated by the client application. For example, the confirmation code can be any number or alphanumeric string. The subscriber is also redirected 212 to the access site by a redirect command that directs the subscriber to the access site. The redirect may also include information that specifically directs the user to a particular server application, and may also include information that allows the access site to automatically respond once the subscriber is navigated to the access site.

(O'Donnell, column 10, lines 18-38)

In this section, O'Donnell describes that when a subscriber wants to access the client application, the client application sends the certificate to the subscriber and the access site. Then, the client application redirects the user to the access site. The user provides the certificate received from the client application to the access site and the access site compares it to a certificate that the access site receives from the client application. Applicants respectfully submit that O'Donnell's access site does not verifying whether the remote command is included in a predefined list stored on the server system. At most, O'Donnell merely compares a certificate from the client application to a certificate from the user. Applicants respectfully submit that one of ordinary skill in the art would not equate a certificate to a remote command. Moreover, O'Donnell merely compares one certificate to another. Nowhere in the O'Donnell reference is there a teaching or suggestion that the certificate from the user is compared to a list of certificates much less a list that includes at least one remote command for satisfying the request of authentication.

Thus, in addition to being dependent on independent claim 1, the specific features of dependent claims 2-7 are also distinguishable over Atkinson, Riggins, and O'Donnell, either alone or in combination, by virtue of the specific features recited in these claims. Accordingly, Applicants respectfully request withdrawal of the rejection of dependent claims 2-7 under 35 U.S.C. § 103(a).

IV. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: February 11, 2008

Francis Lammes
Reg. No. 55,353
WALDER INTELLECTUAL PROPERTY LAW, P.C.
P.O. Box 832745
Richardson, TX 75083
(214) 722-6491
AGENT FOR APPLICANTS